Journal of Pure and Applied Algebra 28 (1983) 235-239
North-Holland

INJECTIVE POLYNOMIAL MAPS AND THE JACOBIAN CONJECTURE

E. CONNELL

The Institute for Advanced Study, Princeton, NJ 08540, and The University of Miami, Coral Gables, FL 33124, USA

L. van den DRIES

The Institute for Advanced Study, Princeton, NJ 08540, and Stanford University, Palo Alto, CA 94305, USA

Communicated by H. Bass
Received 8 December 1982

1. Introduction

Suppose A is an infinite domain and for each i, $i \le i \le n$, $f_i \in A^{[n]} = A[X_1, \dots, X_n] = A[X]$ is a polynomial. Then $f = (f_1, \dots, f_n)$ defines a polynomial map $f: A^n \to A^n$. The Jacobian matrix of f is $J(f) = (\partial f_i / \partial X_j)$, and the statement that the linear part of f is an isomorphism means that the determinant $|J(f)(\mathbf{0})|$ is a unit in A. The first purpose of this paper is to prove the following three theorems.

1.1. Theorem. *Suppose $f: A^n \to A^n$ is a polynomial map whose linear part is an isomorphism, and $a = (a_1, \dots, a_n)$, $c = (c_1, \dots, c_n)$ are distinct points of A^n with $f(a) = f(c)$. Then $(a_1, \dots, a_n, c_1, \dots, c_n)$ is unimodular, that is, this set generates the unit ideal of A. In particular, if $f(a) = f(\mathbf{0})$ and $a \ne \mathbf{0}$, then $(a_1, \dots, a_n)$ is unimodular.*

1.2. Theorem. *Suppose $f: A^n \to A^n$ is a polynomial map with $|J(f)|$ a unit in A, i.e., with $(J(f))$ an invertible matrix. If a and c are distinct points of A^n with $f(a) = f(c)$, and $(x_1, \dots, x_n) \in A^n$, then $(a_1 - x_1, \dots, a_n - x_n, c_1 - x_1, \dots, c_n - x_n)$ is unimodular. In particular, $(a_1 - c_1, \dots, a_n - c_n)$ is unimodular.*

1.3. Theorem. *Suppose $f: A^n \to A^n$ is a polynomial map with $|J(f)|$ a unit in A, $I \subset A$ is a proper ideal, $\bar{A} = A/I$, and the induced map $\bar{f}: (\bar{A})^n \to (\bar{A})^n$ is injective. Then f is injective.*

Now suppose A is a domain of characteristic zero and $f: A^n \to A^n$ is a polynomial map with $f(\mathbf{0}) = \mathbf{0}$, whose linear part is an isomorphism. Let B be the algebraic closure of the field of fractions of A. The degree d of f is the dimension of the field extension $[B(X_1,\dots,X_n):B(f_1,\dots,f_n)]$. Thus the generic fibre of $f:B^n\to B^n$ has d elements ([5] p. 116). For example, $f:\mathbb{R}\to\mathbb{R}$ defined by $f(x)=x+x^3$ has $f'(x)=1+3x^2>0$ and is thus an injective map of degree 3. If $a\in A$, there is defined a polynomial map ${}^af: A^n\to A^n$ (see Section 3 or [2] for the definition). The second purpose of this paper is to prove the following theorem.

1.4. Theorem. *Suppose A is a domain of characteristic zero and $a\in A-0$ is a non-unit, and $f:A^n\to A^n$ is a polynomial map with $f(\mathbf{0})=\mathbf{0}$, whose linear part is an isomorphism. Then ${}^af: A^n\to A^n$ is an injective polynomial map of the same degree as f. Furthermore, ${}^af$ is a polynomial isomorphism iff f is, and $|J({}^af)|$ is a unit of A iff $|J(f)|$ is.*

The Jacobian Conjecture is that if $f:\mathbb{C}^m\to\mathbb{C}^m$ is a polynomial map whose Jacobian matrix has determinant 1, then f is an isomorphism [1]. Let T be the ring of algebraic integers, i.e., the integral closure of $\mathbb{Z}$ in $\mathbb{C}$, and B the field of algebraic numbers, i.e., the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Also let $\wp\subset T$ be a non-zero prime ideal and $A=T_\wp$. The last purpose of this paper is to prove the following theorem.

1.5. Theorem. *If there is a counterexample h to the Jacobian Conjecture, $h:\mathbb{C}^m\to\mathbb{C}^m$, then for some $n>m$, there is a counterexample $f:\mathbb{C}^n\to\mathbb{C}^n$ where the coefficients of each f_i are in $\mathbb{Z}$ and $f:A^n\to A^n$ is injective. Furthermore, it may be assumed that $f_i=x_i+u_i$ where $u_i\in\mathbb{Z}^{[n]}$ is a form of degree 3.*

This is proved in a series of steps. Assume there is a counterexample. We use the Nullstellensatz and the fact that B is an algebraically closed field to show there is a counterexample all of whose coefficients lie in B. Next we carry out a 'Weil Restriction' (Chapter I of [6]) to reduce to the case where the coefficients are in $\mathbb{Q}$. Then the technique of Section 3 is used to clear denominators and obtain coefficients in $\mathbb{Z}$. From [1] it may be assumed that each f_i is of the type $f_i=x_i+u_i$ where $u_i\in\mathbb{Z}^{[n]}$ is a form of degree 3. Finally the technique of Section 3 is used again to construct a counterexample f which is injective on A^n.

2. The proofs of Theorems 1.1, 1.2, and 1.3

If there is a counterexample to Theorem 1.1, then there is a counterexample where A is Noetherian. To see this, suppose $f:A^n\to A^n$ satisfies the hypothesis of 1.1, $a,c\in A^n$ are distinct points with $f(a)=f(c)$, and $I\subset A$ is a maximal ideal with each $a_i,c_i\in I$. Let R be the subring of A generated by the a_i,c_i, the coefficients of each f_i, and the inverse of $|J(f)(\mathbf{0})|$. Then R is a Noetherian ring and $f\,|\,R^n:R^n\to R^n$ is a counterexample to the theorem. Thus it may be assumed that A is Noetherian. Also it may be assumed that $f(\mathbf{0})=\mathbf{0}$.

Now f has a formal power series inverse $g=(g_1,\dots,g_n)$ where $g_i\in A[[X_1,\dots,X_n]]$, and $gf=(g_1(f),\dots,g_n(f))=(X_1,\dots,X_n)$. Let $\hat{A}$ be the I-adic completion of A [4]. Since A is Noetherian, $A\to\hat{A}$ is injective. Each $f_i(a)$ and $f_i(c)$ belongs to I and thus $g(f(a))=g(f(c))$ is a well defined element of $(\hat{A})^n$. However $g(f(a))=a$ and $g(f(c))=c$ and thus $a=c$. This proves Theorem 1.1. Theorem 1.2 follows from 1.1 by translation, and Theorem 1.3 follows immediately from 1.2.

3. The proof of Theorem 1.4

Suppose A is a domain of characteristic zero, $f:A^n\to A^n$ is a polynomial map with $f(\mathbf{0})=\mathbf{0}$, whose linear part is an isomorphism, and $a\in A-0$. Thus $f=(f_1,\dots,f_n)$, $f_i=f_{i,1}+f_{i,2}+\cdots$ where $f_{i,j}\in A^{[n]}$ is a form of degree j. The map ${}^af:A^n\to A^n$ is given by ${}^af_i=f_{i,1}+af_{i,2}+\cdots+a^{t-1}f_{i,t}$. This operation is defined in [2]. In the notation of [3], ${}^af=(Xf)_{x=a}$. If $h:A^n\to A^n$ is another polynomial map with $h(\mathbf{0})=\mathbf{0}$, then ${}^a(hf)={}^ah{}^af$. If the determinant of $J(f)$ is $u_0+u_1+\cdots+u_s$ where $u_i\in A^{[n]}$ is a form of degree i, then the determinant of $J(af)$ is $u_0+au_1+\cdots+a^su_s$. Thus the determinant of $J(f)$ is a unit in A iff the determinant of $J({}^af)$ is.

Let $g=(g_1,\dots,g_n)$ be the formal power series inverse of f, $g_i=g_{i,1}+g_{i,2}+\cdots$ where $g_{i,j}\in A^{[n]}$ is a form of degree j. Then the formal power series inverse of ${}^af$ is ${}^ag$ given by ${}^ag_i=g_{i,1}+ag_{i,2}+a^2g_{i,3}+\cdots$ Since f is a polynomial isomorphism, iff each g_i is a polynomial, f is an isomorphism iff ${}^af$ is.

Now consider $f:B^n\to B^n$ where B is the algebraic closure of the field of fractions of A. Then ${}^af:B^n\to B^n$ is given by ${}^af=h^{-1}fh$ where $h_i(X_1,\dots,X_n)=aX_i$. Since the degree of f is the number of points in the generic fibre, f and ${}^af$ have the same degree.

We are now ready to prove Theorem 1.4. Suppose the hypothesis holds. We will show ${}^af:A^n\to A^n$ is injective. It may be assumed that A is Noetherian. Suppose x and y are distinct points of A^n with ${}^af(x)={}^af(y)$. Since $\bigcap a^iA=0$, there exists an m such that x and y have distinct images in $(A/a^m)^n$. This is impossible because the map $(A/a^m)^n\to(A/a^m)^n$ induced by ${}^af$ is injective, since each ${}^ag_i$ is a polynomial over (A/a^m). This proves ${}^af$ is injective. The rest of Theorem 1.4 follows from the preceding discussion.

4. The proof of Theorem 1.5

Assume that for some integer m, the Jacobian Conjecture is false. We will show that for some integer $n>m$, there is a counterexample $f:\mathbb{C}^n\to\mathbb{C}^n$ such that the coefficients of each f_i lie in $\mathbb{Z}$. Let B be the field of algebraic numbers.

4.1. There exists a counterexample whose coefficients are in B

It follows from [1] and our hypothesis that there exists a polynomial map $h:\mathbb{C}^m \to \mathbb{C}^m$ given by $h_i = x_i +$ higher order, with $|J(h)| = 1$ and $h(1,0,\dots,0) = (0,\dots,0)$. Replace the non-zero coefficients of the monomials of degree ≥ 2 of the h_i by new variables Y_t. Then the determinant of the Jacobian becomes 1 plus some polynomial $p \in \mathbb{Z}[X, Y]$. Each monomial of p in $X_1, \dots, X_m$ has some polynomial $u_i \in \mathbb{Z}[Y]$ as coefficient. The condition $h(1,0,\dots,0) = (0,\dots,0)$ can be expressed as a system of polynomial equations $v_j = 0$ where $v_j \in \mathbb{Z}[Y]$. By hypothesis, the system $u_i = v_j = 0$ has a solution in $\mathbb{C}$. Therefore these polynomials cannot generate the unit ideal in $B[Y]$, and thus by the Nullstellensatz, they have a solution in B.

4.2. There exists a counterexample whose coefficients are in $\mathbb{Q}$

It follows from 4.1 that there is a finite Galois extension K of $\mathbb{Q}$ and a non-injective map $f:K^n \to K^n$ whose Jacobian matrix has determinant 1. More generally, suppose k is a field of characteristic 0, $K \supset k$ is a finite Galois extension of k, and $f:K^n \to K^n$ is a non-injective map whose Jacobian has determinant 1. We show there is a non-injective polynomial map $g:k^{tn} \to k^{tn}$ whose Jacobian has determinant 1, where t is the dimension of K as a vector space over k.

Let $a_1, \dots, a_t$ be a k-basis for K. Introduce new variables $Y_{1,1}, \dots, Y_{t,1}, \dots, Y_{1,n}, \dots, Y_{t,n}$, and let $g_{i,j} \in k[Y_{1,1}, \dots, Y_{t,n}] = k[Y]$ for $1 \leq i \leq t$, $1 \leq j \leq n$ be defined by

$$a_1 g_{1,j} + \cdots + a_t g_{t,j} = f_j(a_1 Y_{1,1} + \cdots + a_t Y_{t,1}, \dots, a_1 Y_{1,n} + \cdots + a_t Y_{t,n}).$$

The desired $g:k^{tn} \to k^{tn}$ is given by $g = (g_{1,1}, \dots, g_{t,1}, \dots, g_{1,n}, \dots, g_{t,n})$. It is immediate that g is not injective and it will be shown that $|J(g)| = 1$.

Now consider g to be a polynomial map $g:K^{tn} \to K^{tn}$. Let

$$h_{in+j} = \sigma_i(a_1) Y_{1,j} + \cdots + \sigma_i(a_t) Y_{t,j} \in K[Y]$$

for $0 \leq i < t$, $1 \leq j \leq n$, where $\sigma_0, \dots, \sigma_{t-1}$ are the Galois automorphisms of K over k. This gives a polynomial map $h:K^{tn} \to K^{tn}$ which is just a linear change of variables. Note that hg is given by polynomials

$$(hg)_{in+j} = h_{in+j}(g_{1,1}, \dots, g_{t,n}) = \sigma_i(a_1) g_{1,j} + \cdots + \sigma_i(a_t) g_{t,j}.$$

If

$$p = \sum c_{s_1, \dots, s_n} X_1^{s_1} \cdots X_n^{s_n} \in K[X_1, \dots, X_n],$$

set

$$p^{\sigma_i} = \sum \sigma_i(c_{s_1, \dots, s_n}) X_{in+1}^{s_1} \cdots X_{(i+1)n}^{s_n} \in K[X_{in+1}, \dots, X_{(i+1)n}].$$

Also set $f^{\sigma_i} = (f_1^{\sigma_i}, \dots, f_n^{\sigma_i})$. This gives a polynomial map

$$\bar{f} = (f^{\sigma_0}, f^{\sigma_1}, \dots, f^{\sigma_{t-1}}) : K^{tn} \to K^{tn}$$

whose Jacobian is

$$\begin{pmatrix} J(f^{\sigma_0}) & & 0 \\ & J(f^{\sigma_1}) \ddots & \\ 0 & & J(f^{\sigma_{t-1}}) \end{pmatrix}.$$

Note that $|J(\bar{f})|=1$ and $(\bar{f}h)_{in+j}=f_j^{\sigma_i}(h)=\sigma_i(a_1)g_{1,j}+\cdots+\sigma_i(a_t)g_{t,j}$ by the defining equation in the second paragraph. Thus $hg=\bar{f}h$, $g=h^{-1}\bar{f}h$, and $J(g)$ has determinant 1.

4.3. *There exists a counterexample whose coefficients are in* $\mathbb{Z}$

It follows from 4.2 that there is a non-injective map $f:\mathbb{Q}^n\to\mathbb{Q}^n$ with $|J(f)|=1$ and $f_i=x_i+f_{i,2}+f_{i,3}+\cdots$. Let t be a positive integer such that $tf_{i,j}\in\mathbb{Z}^{[n]}$. Then ${}^tf=({}^tf_1,\ldots,{}^tf_n)$ is a non-injective map ${}^tf:\mathbb{Q}^n\to\mathbb{Q}^n$ with $|J({}^tf)|=1$ and each ${}^t(f_i)\in\mathbb{Z}^{[n]}$.

From p. 304 of [1], it follows that, for some n, there exists a non-injective map $h:\mathbb{Q}^n\to\mathbb{Q}^n$ with $|J(h)|=1$ and each $h_i=x_i+u_i$ where $u_i\in\mathbb{Z}^{[n]}$ is a form of degree 3.

4.4. *There exists a counterexample which is injective on A*

Recall that B is the field of algebraic numbers, T is the ring of algebraic integers, $\varrho\subset T$ is a non-zero prime ideal, and $A=T_\varrho$. Let p be the prime integer contained in ϱ, and h be as above, $h_i=x_i+u_i$. Define $f=(f_1,\ldots,f_n)$ by $f_i=x_i+p^2u_i$. Then f has coefficients in $\mathbb{Z}$, $|J(f)|=1$, $f:\mathbb{Q}^n\to\mathbb{Q}^n$ is not injective, and $f:A^n\to A^n$ is injective. The generic fibre of $f:B^n\to B^n$ has d elements, where $d>1$ is the degree of f.

It only needs to be shown that f is injective on A^n. This follows from Theorem 1.4 and the fact that $f={}^ph$.

References

[1] H. Bass, E. Connell, and D. Wright, The Jacobian Conjecture: reduction of degree and formal expansion of the inverse, Bull. Amer. Math. Soc. 7 (1982) 287–330.
[2] H. Bass and D. Wright, Localisation in the K-theory of invertible algebras, J. Pure Appl. Algebra 9 (1976) 89–105.
[3] E. Connell, On the K-theory of algebras and polynomial extensions, J. Pure Appl. Algebra 7 (1976) 169–174.
[4] H. Matsumura, Commutative Algebra (Benjamin, New York, 1970).
[5] I.R. Shafarevich, Basic Algebraic Geometry (Springer, New York, 1977).
[6] A. Weil, Adeles and Algebraic Groups, Progress in Math. Vol. 23 (Birkhäuser, Boston, 1982).